New General Secret Sharing Scheme using Hierarchical Threshold Scheme: Improvement of Information Rates for Specified Participants

Kouya Tochikubo
Department of Mathematical Information Engineering, College of Industrial Technology, Nihon University, Japan

Keywords: Secret Sharing Scheme, General Access Structure, $(\mathbf{k},n)$-hierarchical Threshold Scheme, Key Management.

Abstract: In 2015, a new secret sharing scheme realizing general access structures was proposed (T15). This scheme is based on authorized subsets and the first scheme that can reduce the number of shares distributed to specified participants. Reducing the numbers of shares distributed to specified participants is quite useful in secret sharing schemes. However, this scheme needs to use many secret sharing schemes to obtain shares. In this paper, we propose a new secret sharing scheme realizing general access structures. The proposed scheme can reduce the number of secret sharing schemes to obtain shares by using Tassa's $(\mathbf{k},n)$-hierarchical threshold scheme instead of Shamir's (k,n)-threshold scheme. Thus, the proposed scheme is more efficient than the scheme A of T15 from the viewpoint of the number of secret sharing schemes to obtain shares.

1 INTRODUCTION

In (k,n)-threshold scheme (Shamir, 1979; Blakley, 1979), every group of k participants can recover the secret K, but no group of less than k participants can get any information about the secret from their shares. The collection of all authorized subsets of participants is called the access structure. A (k,n)-threshold scheme can only realize particular access structures that contain all subsets of k or more participants. Secret sharing schemes realizing more general access structures than that of a threshold scheme were studied by numerous authors. Subsequently, Tassa proposed a hierarchical threshold scheme using polynomial derivatives (Tassa, 2007).

On the other hand, Ito, Saito and Nishizeki proposed a multiple assignment secret sharing scheme for general access structures and showed an explicit share assignment algorithm for any access structure (Ito et al., 1987). Their scheme can realize an arbitrary access structure by assigning one or more shares to each participant. Benaloh and Leichter proposed a secret sharing scheme for general access structures based on a monotone-circuit (Benaloh and Leichter, 1990). Secret sharing schemes which have an explicit assignment algorithm for any access structure are categorized by two types. One type is schemes based on unauthorized subsets (Ito et al., 1987; Tochikubo, 2004; Tochikubo, 2008). Another type is schemes based on authorized subsets (Benaloh and Leichter, 1990; Tochikubo et al., 2005; Tochikubo, 2013). In this paper, we focus on general secret sharing schemes based on authorized subsets. In the implementation of secret sharing schemes for general access structures, an important issue is the number of shares distributed to each participant. Obviously, a scheme constructed of small shares is desirable. However, in general, the existing secret sharing schemes for general access structures are impractical in this respect when the size of the access structure is very large. Suppose that we want to apply secret sharing schemes to a company. Here, we consider a section which consists of two managers and 20 staff members. A secret can be recovered by a group of two managers or groups of one manager and two staff members. In this case, every manager belongs to 191 minimal authorized subsets and every staff member belongs to 38 minimal authorized subsets. We shall realize this access structure by general secret sharing schemes. Then, each manager has to hold so many shares. In 2015, a new secret sharing scheme realizing general access structures was proposed (T15) (Tochikubo, 2015). This scheme is based on authorized subsets and the first scheme that can reduce the number of shares distributed to specified participants though this scheme cannot reduce the number of shares distributed to every participant. Therefore, reducing the numbers of shares distributed to specified participants is quite useful in secret sharing schemes. However, this scheme needs to use many

Tochikubo, K.
New General Secret Sharing Scheme using Hierarchical Threshold Scheme: Improvement of Information Rates for Specified Participants.
DOI: 10.5220/0009103506470654
In *Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020)*, pages 647-654
ISBN: 978-989-758-399-5; ISSN: 2184-4356

secret sharing schemes to obtain shares.

In this paper, we modify the scheme A of T15 (Tochikubo, 2015) and propose a new secret sharing scheme realizing general access structures. The proposed scheme can reduce the number of secret sharing schemes to obtain shares by using Tassa's $(\mathbf{k},n)$-hierarchical threshold scheme instead of Shamir's (k,n)-threshold scheme. On the other hand, the number of shares distributed to each participant is equal to that of the scheme A of T15. Thus, the proposed scheme is more efficient than the scheme A of T15.

2 PRELIMINARIES

2.1 Secret Sharing Scheme

Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of n participants. Let $D(\notin \mathcal{P})$ denote a dealer who selects a secret and distributes a share to each participant. Let $\mathcal{K}$ and $\mathcal{S}$ denote a secret set and a share set, respectively. For sets A and B, we denote a difference set by $A - B$. The access structure $\Gamma(\subset 2^{\mathcal{P}})$ is the family of subsets of $\mathcal{P}$ which contains the sets of participants qualified to recover the secret. For any authorized subset $A \in \Gamma$, any superset of A is also an authorized subset. Hence, the access structure should satisfy the monotone property:

$$A \in \Gamma, A \subset A' \subset \mathcal{P} \Rightarrow A' \in \Gamma.$$

Let Γ_0 be a family of the minimal sets in Γ, called the minimal access structure. Γ_0 is denoted by

$$\Gamma_0 = \{A \in \Gamma : A' \not\subset A \text{ for all } A' \in \Gamma - \{A\}\}.$$

For any access structure Γ, there is a family of sets $\bar{\Gamma} = 2^{\mathcal{P}} - \Gamma$. $\bar{\Gamma}$ contains the sets of participants unqualified to recover the secret. The family of maximal sets in $\bar{\Gamma}$ is denoted by $\bar{\Gamma}_1$. That is,

$$\bar{\Gamma}_1 = \{B \in \bar{\Gamma} : B \not\subset B' \text{ for all } B' \in \bar{\Gamma} - \{B\}\}.$$

In general, the efficiency of a perfect secret sharing scheme is measured by the information rate ρ (Stinson, 2005) defined as

$$\begin{aligned} \rho &= \min\{\rho_i : 1 \le i \le n\}, \\ \rho_i &= \frac{\log|\mathcal{K}|}{\log|\mathcal{S}(P_i)|} \end{aligned}$$

where $\mathcal{S}(P_i)$ denotes the set of possible shares that P_i might receive. Obviously, a high information rate is desirable. Throughout the paper, p is a large prime, and let Z_p be a finite field with p elements. In this paper, we assume $\mathcal{K} = \mathcal{S} = Z_p$.

2.2 Shamir's Threshold Scheme

Shamir's (k,n)-threshold scheme is described as follows (Shamir, 1979):

1. A dealer D chooses n distinct nonzero elements of Z_p, denoted by $x_1, x_2, \cdots, x_n$. The values x_i are public.
2. Suppose D wants to share a secret $K \in Z_p$, D chooses $k-1$ elements $a_1, a_2, \cdots a_{k-1}$ from Z_p independently with the uniform distribution.
3. D distributes the share $s_i = f(x_i)$ to P_i $(1 \le i \le n)$, where

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$$

is a polynomial over Z_p.

It is known that Shamir's (k,n)-threshold scheme is perfect and ideal (Stinson, 2005; Karnin et al., 1983). This implies that every k participants can recover the secret K, but no group of less than k participants can get any information about the secret.

The access structure of (k,n)-threshold scheme is described as follows:

$$\Gamma = \{A \in 2^{\mathcal{P}} : |A| \ge k\}.$$

2.3 Tassa's Hierarchical Threshold Scheme

Let $\mathcal{P}$ be a set of n participants and assume that $\mathcal{P}$ is divided into $m+1$ disjoint subsets $\mathcal{U}_0, \mathcal{U}_2, \cdots, \mathcal{U}_m$, i.e.

$$\mathcal{P} = \bigcup_{i=0}^{m} \mathcal{U}_i \text{ and } \mathcal{U}_i \cap \mathcal{U}_j = \phi \text{ for all } 0 \le i < j \le m.$$

Let $\mathbf{k} = \{k_i\}_{i=0}^{m}$ be a monotonically increasing sequence of integers $0 < k_0 < \cdots < k_m$. We set $k = k_m$. Tassa's $(\mathbf{k},n)$-hierarchical threshold scheme is described as follows (Tassa, 2007):

1. Suppose A dealer D wants to share a secret $K \in Z_p$, D chooses $k-1$ elements $a_1, a_2, \cdots a_{k-1}$ from Z_p independently with the uniform distribution and defines a polynomial over Z_p

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}.$$

2. D identifies each participant $P \in \mathcal{P}$ with a field element. For simplicity, the field element that corresponds to $P_r \in \mathcal{P}$ will be also denoted by r $(1 \le r \le n)$.

3. D distributes the shares to all participants in the following manner: Each participant of i th level in the hierarchy $P_r \in \mathcal{U}_i$ receives the share $f^{(k_{i-1})}(r)$ where $f^{(k_{i-1})}(r)$ denotes the (k_{i-1}) th derivative of $f(x)$ at $x = r$ and $k_{-1} = 0$.

The access structure of Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme is described as follows:

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{P} : \left| \mathcal{V} \cap \left(\bigcup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i, \quad \forall i \in \{0, 1, \ldots, m\} \right\}.$$

It is known that Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme is perfect and ideal (Tassa, 2007).

Example 1: Let $\mathbf{k} = (k_0, k_1, k_2) = (1, 3, 4)$, $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ and

$$\begin{aligned} \mathcal{U}_0 &= \{P_1\}, \\ \mathcal{U}_1 &= \{P_2, P_3, P_4\}, \\ \mathcal{U}_2 &= \{P_5, P_6\}. \end{aligned}$$

In this case, the access structure Γ and the minimal access structure Γ_0 of Tassa's $((1,3,4),6)$-hierarchical threshold scheme are described by

$$\Gamma = \left\{ \mathcal{V} \subset \mathcal{P} : \left| \mathcal{V} \cap \left(\bigcup_{j=0}^{i} \mathcal{U}_j \right) \right| \geq k_i, \forall i \in \{0, 1, 2\} \right\}$$

and

$$\begin{aligned} \Gamma_0 = \{ &\{P_1, P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_5\}, \\ &\{P_1, P_2, P_3, P_6\}, \{P_1, P_2, P_4, P_5\}, \\ &\{P_1, P_2, P_4, P_6\}, \{P_1, P_3, P_4, P_5\}, \\ &\{P_1, P_3, P_4, P_6\}\}, \end{aligned}$$

respectively. Here, we shall realize this access structure by Tassa's scheme.

1. D selects a random polynomial
$$f(x) = K + a_1 x + a_2 x^2 + a_3 x^3.$$
2. D distributes the share $s_1 = f(1)$ to P_1.
3. D distributes the share $s_r = f'(r)$ to P_r $(2 \leq r \leq 4)$, where
$$f'(x) = a_1 + 2a_2 x + 3a_3 x^2.$$
4. D distributes the share $s_r = f^{(3)}(r)$ to P_r $(5 \leq r \leq 6)$, where
$$f^{(3)}(x) = 6a_3.$$

Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme can realize more general access structures than that of a threshold scheme. If $i = 0$, then Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme coincides Shamir's (k, n)-threshold scheme.

2.4 Secret Sharing Schemes based on Authorized Subsets

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $K \in \mathcal{K}$ and Γ, Benaloh and Leichter's scheme is described as follows (Benaloh and Leichter, 1990):

1. Let $\Gamma_0 = \{A_1, A_2, \cdots, A_m\}$. For $A_i \in \Gamma_0$, compute $|A_i|$ shares $s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$ by using an $(|A_i|, |A_i|)$-threshold scheme with K as a secret independently for $1 \leq i \leq m$.
2. One distinct share from $s_{i,1}, s_{i,2}, \cdots, s_{i,|A_i|}$ is assigned to each $P \in A_i$ $(1 \leq i \leq m)$.

Example 2: For $\mathcal{P} = \{P_1, P_2, P_3, P_4, P_5, P_6\}$, consider the following access structure

$$\Gamma_0 = \{A_1, A_2, \cdots, A_6\}$$

where

$$\begin{aligned} A_1 &= \{P_1, P_2, P_5, P_6\}, \\ A_2 &= \{P_2, P_3, P_5, P_6\}, \\ A_3 &= \{P_2, P_4, P_5, P_6\}, \\ A_4 &= \{P_3, P_4, P_5, P_6\}, \\ A_5 &= \{P_1, P_2, P_3, P_4, P_5\}, \\ A_6 &= \{P_1, P_2, P_3, P_4, P_6\}. \end{aligned}$$

We shall realize this access structure by Benaloh and Leichter's scheme. In this case, shares are distributed as follows:

$$\begin{aligned} P_1 &: s_{1,1}, s_{5,1}, s_{6,1} \\ P_2 &: s_{1,2}, s_{2,1}, s_{3,1}, s_{5,2}, s_{6,2} \\ P_3 &: s_{2,2}, s_{4,1}, s_{5,3}, s_{6,3} \\ P_4 &: s_{3,2}, s_{4,2}, s_{5,4}, s_{6,4} \\ P_5 &: s_{1,3}, s_{2,3}, s_{3,3}, s_{4,3}, s_{5,5} \\ P_6 &: s_{1,4}, s_{2,4}, s_{3,4}, s_{4,4}, s_{6,5} \end{aligned}$$

where $s_{i,j}$ is computed by using Shamir's $(|A_i|, |A_i|)$-threshold scheme with K as a secret $(1 \leq i \leq 6,\ 1 \leq j \leq |A_i|)$.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $Q(\subset \mathcal{P})$, $K \in \mathcal{K}$ and Γ, the scheme A of T15 is described as follows (Tochikubo, 2015):

1. Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C \text{ for some } A \in \Gamma_0\}$ and represent it as $\mathcal{A}' = \{C'_1, C'_2, \cdots, C'_m\}$.
2. For $C'_i \in \mathcal{A}'$, let
$$\begin{aligned} \mathcal{A}_i = \{ &B \subset \mathcal{P} - Q : B \cap C'_i = \phi \\ &\text{and } B \cup C'_i = A \text{ for some } A \in \Gamma_0\} \end{aligned}$$
and represent it as $\mathcal{A}_i = \{C_{i1}, C_{i2}, \cdots, C_{i|\mathcal{A}_i|}\}$.

3. For $C'_i \in \mathcal{A}'$,
   (i) if $C'_i = \phi$ then $S_i = \{w_i\}$ and $w_i = K$,
   (ii) if $C'_i \neq \phi$ and $\mathcal{A}_i = \{\phi\}$ then $S_i = \{w'_i\}$ and $w'_i = K$,
   (iii) if $C'_i \neq \phi$ and $\mathcal{A}_i \neq \{\phi\}$ then compute 2 shares $S_i = \{w_i, w'_i\}$ by using Shamir's $(2,2)$-threshold scheme with K as a secret for $1 \leq i \leq m$.
4. For $C'_i \in \mathcal{A}'$, if $C'_i = \phi$ then $S_{1,i} = \phi$, else compute $|C'_i|$ shares
$$S_{1,i} = \{s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|C'_i|}\}$$
by using Shamir's $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret for $1 \leq i \leq m$. One distinct share in $S_{1,i}$ is assigned to each $P \in C'_i$ $(1 \leq i \leq m)$.
5. For $C_{ij} \in \mathcal{A}_i$, if $C_{ij} = \phi$ then $S_{2,i,j} = \phi$, else compute $|C_{ij}|$ shares
$$S_{2,i,j} = \{s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}\}$$
by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret for $1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|$. One distinct share in $S_{2,i,j}$ is assigned to each $P \in C_{ij}$ $(1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|)$.

Example 3: Let $Q = \{P_1, P_2\}$. We shall realize the access structure of Example 2 by the scheme A of T15.

- Since $Q = \{P_1, P_2\}$, $\mathcal{A}'$ is defined by
$$\mathcal{A}' = \{C'_1, C'_2, C'_3\}$$
where
$$\begin{aligned} C'_1 &= \{P_1, P_2\}, \\ C'_2 &= \{P_2\}, \\ C'_3 &= \phi. \end{aligned}$$
- $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are defined by
$$\begin{aligned} \mathcal{A}_1 &= \{\{P_5, P_6\}, \{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}\}, \\ \mathcal{A}_2 &= \{\{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}\}, \\ \mathcal{A}_3 &= \{\{P_3, P_4, P_5, P_6\}\}. \end{aligned}$$
- For $C'_1, C'_2 \in \mathcal{A}'$, compute 2 shares
$$\begin{aligned} S_1 &= \{w_1, w'_1\}, \\ S_2 &= \{w_2, w'_2\} \end{aligned}$$
by using Shamir's $(2,2)$-threshold scheme with K as a secret. Since $C'_3 = \phi$, we set
$$S_3 = \{w_3\} \text{ and } w_3 = K.$$
- For $C'_1, C'_2 \in \mathcal{A}'$, compute $|C'_i|$ shares
$$\begin{aligned} S_{1,1} &= \{s'_{1,1}, s'_{1,2}\}, \\ S_{1,2} &= \{s'_{2,1}\} \end{aligned}$$
by using $(|C'_i|, |C'_i|)$-threshold scheme with w'_i as a secret independently for $1 \leq i \leq 2$. Since $C'_3 = \phi$, we set
$$S_{1,3} = \phi.$$
- For $C_{ij} \in \mathcal{A}_i$, compute $|C_{ij}|$ shares
$$\begin{aligned} S_{2,1,1} &= \{s_{1,1,1}, s_{1,1,2}\}, \\ S_{2,1,2} &= \{s_{1,2,1}, s_{1,2,2}, s_{1,2,3}\}, \\ S_{2,1,3} &= \{s_{1,3,1}, s_{1,3,2}, s_{1,3,3}\}, \\ S_{2,2,1} &= \{s_{2,1,1}, s_{2,1,2}, s_{2,1,3}\}, \\ S_{2,2,2} &= \{s_{2,2,1}, s_{2,2,2}, s_{2,2,3}\}, \\ S_{2,3,1} &= \{s_{3,1,1}, s_{3,1,2}, s_{3,1,3}, s_{3,1,4}\} \end{aligned}$$
by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with w_i as a secret independently for $1 \leq i \leq 3, 1 \leq j \leq |\mathcal{A}_i|$.
- In this case, shares are distributed as follows:
$$\begin{aligned} P_1 &: s'_{1,1} \\ P_2 &: s'_{1,2}, s'_{2,1} \\ P_3 &: s_{1,2,1}, s_{1,3,1}, s_{2,1,1}, s_{3,1,1} \\ P_4 &: s_{1,2,2}, s_{1,3,2}, s_{2,2,1}, s_{3,1,2} \\ P_5 &: s_{1,1,1}, s_{1,2,3}, s_{2,1,2}, s_{2,2,2}, s_{3,1,3} \\ P_6 &: s_{1,1,2}, s_{1,3,3}, s_{2,1,3}, s_{2,2,3}, s_{3,1,4}. \end{aligned}$$

Benaloh and Leichter's scheme needs shares for each minimal authorized subset. On the other hand, the scheme A of T15 can reduce the number of shares distributed to each participant $P \in Q(\subset \mathcal{P})$.

3 PROPOSED SCHEME

Here, we propose a new secret sharing scheme realizing general access structures. In the proposed scheme, we can select a subset of participants $Q(\subset \mathcal{P})$ without restrictions. The proposed scheme can reduce the number of shares distributed to $P \in Q$ by dividing Γ_0 into $\mathcal{A}_1, \mathcal{A}_2, \cdots, \mathcal{A}_m$ according to the subsets of Q in the same way as the scheme A of T15. The proposed scheme can reduce the number of secret sharing schemes to obtain shares by using Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme instead of Shamir's (k,n)-threshold scheme. On the other hand, the number of shares distributed to each participant is equal to that of the scheme A of T15.

For $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$, $Q(\subset \mathcal{P})$, $K \in \mathcal{K}$ and Γ, the proposed scheme is described as follows:

1. Let $\mathcal{A}' = \{C \subset Q : Q \cap A = C \text{ for some } A \in \Gamma_0\}$ and represent it as $\mathcal{A}' = \{C'_1, C'_2, \cdots, C'_m\}$.
2. For $C'_i \in \mathcal{A}'$, let

$$\begin{aligned}\mathcal{A}_i &= \{B \subset \mathcal{P} - Q : B \cap C'_i = \phi \\ &\qquad \text{and } B \cup C'_i = A \text{ for some } A \in \Gamma_0\}\end{aligned}$$

and represent it as $\mathcal{A}_i = \{C_{i1}, C_{i2}, \cdots, C_{i|\mathcal{A}_i|}\}$.

3. For $C'_i \in \mathcal{A}'$,

(i) if $C'_i = \phi$ then set

$$S_{1,i} = \phi, S_{2,i} = \{s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|\mathcal{A}_i|}\}$$

where $s'_{i,j} = K (1 \le j \le |\mathcal{A}_i|)$,

(ii) if $C'_i \neq \phi$ and $\mathcal{A}_i = \{\phi\}$ then compute $|C'_i|$ shares

$$S_{1,i} = \{s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|C'_i|}\}$$

by using Shamir's $(|C'_i|, |C'_i|)$-threshold scheme with K as a secret,

(iii) if $C'_i \neq \phi$ and $\mathcal{A}_i \neq \{\phi\}$ then by using Tassa's $((|C'_i|, |C'_i|+1), |C'_i| + |\mathcal{A}_i|)$-hierarchical threshold scheme with K as a secret, compute $|C'_i| + |\mathcal{A}_i|$ shares

$$S_{1,i} = \{s'_{i,|\mathcal{A}_i|+1}, \cdots, s'_{i,|\mathcal{A}_i|+|C'_i|}\},$$
$$S_{2,i} = \{s'_{i,1}, s'_{i,2}, \cdots, s'_{i,|\mathcal{A}_i|}\}$$

as follows:

$$s'_{i,j} = \begin{cases} f(j) & (|\mathcal{A}_i| + 1 \le j \le |\mathcal{A}_i| + |C'_i|) \\ f^{(|C'_i|)}(j) & (1 \le j \le |\mathcal{A}_i|). \end{cases}$$

One distinct share in $S_{1,i}$ is assigned to each $P \in C'_i$ $(1 \le i \le m)$.

4. For $C_{ij} \in \mathcal{A}_i$, if $C_{ij} = \phi$ then $S_{2,i,j} = \phi$, else compute $|C_{ij}|$ shares

$$S_{2,i,j} = \{s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}\}$$

by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with $s'_{i,j}$ as a secret for $1 \le i \le m, 1 \le j \le |\mathcal{A}_i|$. One distinct share in $S_{2,i,j}$ is assigned to each $P \in C_{ij}$ $(1 \le i \le m, 1 \le j \le |\mathcal{A}_i|)$.

Example 4: Let $Q = \{P_1, P_2\}$. We shall realize the access structure of Example 2 by the proposed scheme.

- Since $Q = \{P_1, P_2\}$, $\mathcal{A}'$ is defined by $\mathcal{A}' = \{C'_1, C'_2, C'_3\}$ where

$$\begin{aligned} C'_1 &= \{P_1, P_2\}, \\ C'_2 &= \{P_2\}, \\ C'_3 &= \phi. \end{aligned}$$

- $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are defined by

$$\begin{aligned} \mathcal{A}_1 &= \{\{P_5, P_6\}, \{P_3, P_4, P_5\}, \{P_3, P_4, P_6\}\}, \\ \mathcal{A}_2 &= \{\{P_3, P_5, P_6\}, \{P_4, P_5, P_6\}\}, \\ \mathcal{A}_3 &= \{\{P_3, P_4, P_5, P_6\}\}. \end{aligned}$$

- For $C'_1, C'_2 \in \mathcal{A}'$, compute $|C'_i| + |\mathcal{A}_i|$ shares

$$\begin{aligned} S_{1,1} &= \{s'_{1,4}, s'_{1,5}\}, \\ S_{1,2} &= \{s'_{1,1}, s'_{1,2}, s'_{1,3}\}, \\ S_{2,1} &= \{s'_{2,3}\}, \\ S_{2,2} &= \{s'_{2,1}, s'_{2,2}\} \end{aligned}$$

by using Tassa's $((|C'_i|, |C'_i|+1), |C'_i| + |\mathcal{A}_i|)$-hierarchical threshold scheme with K as a secret $(1 \le i \le 2)$. Since $C'_3 = \phi$, we set $S_{1,3} = \phi, S_{2,3} = \{s'_{3,1}\}$ where $s'_{3,1} = K$

- For $C_{ij} \in \mathcal{A}_i$, compute $|C_{ij}|$ shares

$$\begin{aligned} S_{2,1,1} &= \{s_{1,1,1}, s_{1,1,2}\}, \\ S_{2,1,2} &= \{s_{1,2,1}, s_{1,2,2}, s_{1,2,3}\}, \\ S_{2,1,3} &= \{s_{1,3,1}, s_{1,3,2}, s_{1,3,3}\}, \\ S_{2,2,1} &= \{s_{2,1,1}, s_{2,1,2}, s_{2,1,3}\}, \\ S_{2,2,2} &= \{s_{2,2,1}, s_{2,2,2}, s_{2,2,3}\}, \\ S_{2,3,1} &= \{s_{3,1,1}, s_{3,1,2}, s_{3,1,3}, s_{3,1,4}\} \end{aligned}$$

by using Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with $s'_{i,j}$ as a secret for $1 \le i \le 3, 1 \le j \le |\mathcal{A}_i|$.

- In this case, shares are distributed as follows:

$$\begin{aligned} P_1 &: s'_{1,4} \\ P_2 &: s'_{1,5}, s'_{2,3} \\ P_3 &: s_{1,2,1}, s_{1,3,1}, s_{2,1,1}, s_{3,1,1} \\ P_4 &: s_{1,2,2}, s_{1,3,2}, s_{2,2,1}, s_{3,1,2} \\ P_5 &: s_{1,1,1}, s_{1,2,3}, s_{2,1,2}, s_{2,2,2}, s_{3,1,3} \\ P_6 &: s_{1,1,2}, s_{1,3,3}, s_{2,1,3}, s_{2,2,3}, s_{3,1,4}. \end{aligned}$$

The next theorem shows the proposed scheme is perfect.

Theorem 1. *Let $\mathcal{P} = \{P_1, P_2, \cdots, P_n\}$ be a set of n participants. For any $Q(\subset \mathcal{P})$ and any access structure $\Gamma(\subset 2^{\mathcal{P}})$, distribute shares for a secret K by using the proposed scheme A. Then, for any subset $X \subset \mathcal{P}$,*

(a) $X \in \Gamma \Rightarrow H(K|X) = 0$,
(b) $X \notin \Gamma \Rightarrow H(K|X) = H(K)$.

Proof: Let $X_{S_{1,i}}$ and $X_{S_{2,i,j}}$ denote the shares in $S_{1,i}$ and $S_{2,i,j}$ assigned to X, respectively$(1 \le i \le m, 1 \le j \le |\mathcal{A}_i|)$. At first, we show $H(K|X) = 0$ for any $X \in$

Γ. From the property of the access structure and the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, there exists $A \in \Gamma_0$ such that

$$C'_i \cup C_{ij} = A \subset X.$$

In this case, we have

$$|X_{S_{1,i}}| = |C'_i| \text{ and } |X_{S_{2,i,j}}| = |C_{ij}|.$$

Since $s_{i,j,1}, s_{i,j,2}, \cdots, s_{i,j,|C_{ij}|}$ are shares computed by Shamir's $(|C_{ij}|, |C_{ij}|)$-threshold scheme with $s'_{i,j}$ as a secret, X can recover $s'_{i,j}$ if $C_{ij} \neq \phi$. From the definition of $S_{1,i}$, $S_{2,i}$ and $S_{2,i,j}$, we immediately obtain

$$\begin{aligned} & H(K|X) \\ &= H(K|X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\ &\leq H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) \\ &= 0. \end{aligned}$$

Since $H(K|X) \geq 0$ is obvious, we have $H(K|X) = 0$ for any $X \in \Gamma$.

Next we show $H(K|X) = H(K)$ for any $X \notin \Gamma$. From the property of the access structure and the definition of $\mathcal{A}_i, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, for any $A_i \in \Gamma_0$, we have

$$C'_i \not\subset X \text{ or } C_{ij} \not\subset X \ (1 \leq j \leq |\mathcal{A}_i|).$$

This implies

$$H(K|X_{S_{1,i}}, X_{S_{2,i,j}}) = H(K).$$

for $1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|$. From the definition of $S_{1,i}$, $S_{2,i}$ and $S_{2,i,j}$, we have

$$H(K|X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}) = H(K)$$

for $1 \leq i \leq m$. This implies

$$\begin{aligned} & H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}|K) \\ &= H(X_{S_{1,i}}, X_{S_{2,i,1}}, \cdots, X_{S_{2,i,|\mathcal{A}_i|}}). \end{aligned} \quad (1)$$

In order to show $H(K|X) = H(K)$, we expand $H(K|X)$ as follows:

$$\begin{aligned} & H(K|X) \\ &= H(K|X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\ &= H(K) \\ &\quad + H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}|K) \\ &\quad - H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}). \end{aligned} \quad (2)$$

From the chain rule for entropy, we have

$$\begin{aligned} & H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}|K) \\ &= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|K, X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\ &\overset{(*)}{=} \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|K) \\ &= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \end{aligned} \quad (3)$$

Here, $(*)$ comes from the fact that $X_{S_{1,1}}, \cdots, X_{S_{1,m}}$ and $X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}$ are mutually independent and the last equality comes from (1). On the other hand, we have

$$\begin{aligned} & H(X_{S_{1,1}}, \cdots, X_{S_{1,m}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,m,|\mathcal{A}_m|}}) \\ &= \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}|X_{S_{1,1}}, \cdots \\ &\qquad \cdots, X_{S_{1,t-1}}, X_{S_{2,1,1}}, \cdots, X_{S_{2,t-1,|\mathcal{A}_{t-1}|}}) \\ &\leq \sum_{t=1}^{m} H(X_{S_{1,t}}, X_{S_{2,t,1}}, \cdots, X_{S_{2,t,|\mathcal{A}_t|}}). \end{aligned} \quad (4)$$

Substituting (3) and (4) into (2), we obtain $H(K|X) \geq H(K)$. Since $H(K|X) \leq H(K)$ is obvious, we have $H(K|X) = H(K)$. □

4 EVALUATION OF THE EFFICIENCY

The number of shares distributed to $P \in \mathcal{P}$ for the access structure of Example are described in Table 1.

Table 1: Comparison of the number of shares distributed to $P \in \mathcal{P}$.

	P_1	P_2	P_3	P_4	P_5	P_6
Scheme of BL88	3	5	4	4	5	5
Scheme A of T15	1	2	4	4	5	5
Proposed scheme	1	2	4	4	5	5

This result shows that the proposed scheme and the scheme A of T15 can reduce the numbers of shares distributed to $P \in Q$.

Let $N(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using the proposed scheme. Similarly, let $N_{BL}(P)$ and $N_{T15_A}(P)$ be the number of shares distributed to $P \in \mathcal{P}$ by using Benaloh and Leichter's scheme and the scheme A of T15, respectively. The next theorem shows the number of shares distributed to each participant is equal to that of the scheme A of T15 in the proposed scheme and the proposed scheme is more efficient than Benaloh and Leichter's scheme and from the viewpoint of the number of shares distributed to each participant.

Theorem 2. *For any $P \in \mathcal{P}$, the number of shares distributed to P is evaluated as follows:*

$$N(P) = \begin{cases} N_{BL}(P) - \sum_{i=1}^{m} |\{P\} \cap C'_i|(|\mathcal{A}_i| - 1) & (P \in Q) \\ N_{BL}(P) & (P \notin Q), \end{cases}$$

$$N(P) = N_{T15_A}(P) \ \ (P \in \mathcal{P}).$$

Proof: From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, $N(P)$ and $N_{T15_A}(P)$ are obtained by

$$N(P) = N_{T15_A}(P) = |\{C' \in \mathcal{A}' : P \in C'\}| = \sum_{i=1}^{m} |\{P\} \cap C'_i| \quad (5)$$

for $P \in Q$. On the other hand, $N_{BL}(P)$ is obtained by

$$N_{BL}(P) = |\{X \in \Gamma_0 : P \in X\}|. \quad (6)$$

From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, we have

$$\{X \in \Gamma_0 : P \in X\} = \bigcup_{i=1}^{m} \{C'_i \cup C : P \in C'_i, C \in \mathcal{A}_i\} \quad (7)$$

for $P \in Q$. From (6) and (7), we have

$$N_{BL}(P) = \sum_{i=1}^{m} |\{C'_i \cup C : P \in C'_i, C \in \mathcal{A}_i\}| = \sum_{i=1}^{m} |\{P\} \cap C'_i| \cdot |\mathcal{A}_i| \quad (8)$$

for $P \in Q$.

Similarly, $N(P)$ and $N_{T15_A}(P)$ are obtained by

$$N(P) = N_{T15_A}(P) = \sum_{i=1}^{m} |\{C \in \mathcal{A}_i : P \in C\}| \quad (9)$$

for $P \notin Q$. From the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, we have

$$\{X \in \Gamma_0 : P \in X\} = \bigcup_{i=1}^{m} \{C'_i \cup C : P \in C \in \mathcal{A}_i\} \quad (10)$$

for $P \notin Q$. From (6) and (10), we have

$$N_{BL}(P) = \sum_{i=1}^{m} |\{C'_i \cup C : P \in C \in \mathcal{A}_i\}| = \sum_{i=1}^{m} |\{C \in \mathcal{A}_i : P \in C\}| \quad (11)$$

for $P \notin Q$. Theorem 2 is easily obtained by (5), (8), (9) and (11). □

Here, we evaluate the number of secret sharing schemes to obtain shares. Table 2 shows the number of secret sharing schemes to obtain shares for Example.

This result shows that the proposed scheme can reduce the number of secret sharing schemes to obtain shares. Actually, we can reduce $|\mathcal{A}' - \{\phi\}|$ secret sharing schemes at most.

Let N' be the number of secret sharing schemes to obtain shares in the proposed scheme. Similarly, let N'_{BL} and N'_{T15_A} be the number of secret sharing schemes to obtain shares in Benaloh and Leichter's scheme and the scheme A of T15, respectively.

Table 2: Comparison of the number of secret sharing schemes.

	Shamir's schemes	Tassa's schemes	total
Scheme of BL88	6	0	6
Scheme A of T15	10	0	10
Proposed scheme	6	2	8

The next theorem shows the proposed scheme is more efficient than the scheme A of T15 from the viewpoint of the number of secret sharing schemes to obtain shares.

Theorem 3. *The number of secret sharing schemes to obtain shares is evaluated as follows:*

$$N'_{BL} = |\Gamma_0|,$$
$$N'_{T15_A} \leq |\Gamma_0| + 2|\mathcal{A}' - \{\phi\}|,$$
$$N' \leq |\Gamma_0| + |\mathcal{A}' - \{\phi\}|.$$

Proof: Benaloh and Leichter's scheme uses secret sharing schemes for each minimal authorized subset A_i in Γ_0. Thus, we have

$$N'_{BL} = |\Gamma_0|.$$

The scheme A of T15 uses secret sharing schemes for each C'_i in $\mathcal{A}' - \{\phi\}$ to obtain S_i $(1 \leq i \leq m)$, C'_i in $\mathcal{A}' - \{\phi\}$ to obtain $S_{1,i}$ $(1 \leq i \leq m)$ and C_{ij} in $\mathcal{A}_i$ to obtain $S_{2,i,j}(1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|)$. The proposed scheme uses secret sharing schemes for each C'_i in $\mathcal{A}' - \{\phi\}$ to obtain $S_{1,i}$ and $S_{2,i}$ $(1 \leq i \leq m)$ and C_{ij} in $\mathcal{A}_i - \{\phi\}$ to obtain $S_{2,i,j}(1 \leq i \leq m, 1 \leq j \leq |\mathcal{A}_i|)$.

On the other hand, from the definition of $\mathcal{A}_1, \cdots, \mathcal{A}_m$ and $\mathcal{A}'$, we have

$$\sum_{i=1}^{m} |\mathcal{A}_i| \leq |\Gamma_0|.$$

Thus, we obtain

$$N'_{T15_A} \leq |\Gamma_0| + 2|\mathcal{A}' - \{\phi\}|,$$
$$N' \leq |\Gamma_0| + |\mathcal{A}' - \{\phi\}|.$$

□

5 CONCLUSION

We have proposed a new secret sharing scheme realizing general access structures. The proposed scheme can reduce the number of secret sharing schemes to obtain shares by using Tassa's $(\mathbf{k}, n)$-hierarchical threshold scheme instead of Shamir's (k, n)-threshold scheme. On the other hand, the number of shares distributed to each participant is equal to that of the scheme A of T15.

ACKNOWLEDGEMENTS

This work was supported by JSPS KAKENHI Grant Number 18K11303.

REFERENCES

Benaloh, J. and Leichter, J. (1990). Generalized secret sharing and monotone functions. In *Proceedings on Advances in Cryptology*, CRYPTO '88, pages 27–35, Berlin, Heidelberg. Springer-Verlag.

Blakley, G. R. (1979). Safeguarding cryptographic keys. In *1979 International Workshop on Managing Requirements Knowledge (MARK)*, pages 313–318.

Ito, M., Saito, A., and Nishizeki, T. (1987). Secret sharing scheme realizing general access structure. In *Proc. IEEE Globecom'87*, pages 99–102.

Karnin, E., Greene, J., and Hellman, M. (1983). On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41.

Shamir, A. (1979). How to share a secret. *Commun. ACM*, 22(11):612–613.

Stinson, D. R. (2005). *Cryptography: theory and practice*. CRC Press, 3rd edition.

Tassa, T. (2007). Hierarchical threshold secret sharing. *Journal of Cryptology*, 20:237–264.

Tochikubo, K. (2004). Efficient secret sharing schemes realizing general access structures. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E87-A(7):1788–1797.

Tochikubo, K. (2008). Efficient secret sharing schemes based on unauthorized subsets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E91-A(10):2860–2867.

Tochikubo, K. (2013). New construction methods of secret sharing schemes based on authorized subsets. *Information and Media Technologies*, 8(4):978–986.

Tochikubo, K. (2015). New secret sharing schemes realizing general access structures. *Journal of Information Processing*, 23(5):570–578.

Tochikubo, K., Uyematsu., T., and Matsumoto, R. (2005). Efficient secret sharing schemes based on authorized subsets. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E88-A:322–326.